

REMARKS

Claims 1 to 20 are now pending. Claims 1, 6, 7 and 11 have been amended to correct any minor informalities. New claim 20 has been added. Support for such can be found throughout the Specification. No new matter has been added. Above, any amendments to the claims are shown by underlining (additions) and strikeout (deletions).

Applicants respectfully request reconsideration of the present application in view of this response.

In a previous Office Action, claims 1 to 3, 7 to 11, 13, 14, 18 and 19 were rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 6,052,466 to Wright (the “Wright reference”) in view of U.S. Patent No. 5,778,072 to Samar (the “Samar reference”).

The Wright reference purportedly concerns an encryption of data packets using a sequence of private keys generated from a public key exchange. See Title. The Wright reference refers to partitioning a first cipher stream generated from a private key negotiated as a result of a public key exchange to form a sequence of secondary keys, and indexing the secondary keys. See Abstract, lines 1-4. The Wright reference further refers to encrypting each plaintext data packet with a second cipher stream generated from a different one of the secondary keys, or to using a second cipher stream generated from a single secondary key to encrypt a plurality of plaintext data packets. Abstract, lines 4-8. The Wright reference further refers to using a new second cipher stream generated from another one of the secondary keys for encryption following each instance of the loss of a ciphertext data packet. Abstract, lines 8-11. The Wright reference refers to communication an index with the ciphertext to identify which secondary key is to be used in generating the second cipher stream needed for decryption; and, with knowledge of the secondary key to be used, resynchronization (along with new private key negotiation) at each instance of a ciphertext data packet loss is obviated. Abstract, lines 11-17.

Amended claim 1 involves a method for secure transmission of messages between at least two users of a telecommunications network and recites:

*providing a secret random binary encryption key provided by a key generator;
recording the key on a first portable medium and a second portable medium*

so as to define a first and a second recorded key, a first user of the at least two users receiving the first portable medium with the first recorded key and a second user of the at least two users receiving the second portable medium with the second recorded key;

inserting the first medium into a first reading device assigned to a first telecommunications device of the telecommunications network and inserting the second medium into a second reading device assigned to a second telecommunications device of the telecommunications network, and reading the first and second recorded keys using the first and second reading devices respectively; establishing a connection between the first and second telecommunications devices;

checking the inserting and comparing the first and second recorded keys using a first logistics device and a second logistics device, the first logistics device being assigned to the first telecommunications device and the second logistics device being assigned to the second telecommunications device; and upon a match in the comparing, encrypting the messages using at least a part of the key.

In contrast, the Wright reference does not teach or even suggest providing a secret random binary encryption key provided by a key generator and recording the key on a first portable medium and a second portable medium so as to define a first and a second recorded key, a first user of the at least two users receiving the first portable medium with the first recorded key and a second user of the at least two users receiving the second portable medium with the second recorded key, as in claim 1. Instead, the Wright reference purportedly concerns an encryption system utilizing four values: a secret random quantity y , a public based vector a , a public modulus p , and a public key PK calculated with the equation at col. 2, lines 20-23. The Wright reference refers to each party having its own secret random quantity y and calculates its own public key PK . The Wright reference further refers to the three values a , p , and PK being exchanged prior to any encrypted communications. The Wright reference also refers to both parties independently calculating a shared private key K with equations (4) and (5) at col. 2, line 6 to col. 3, line 5. The Wright reference refers to having the private key

used by a cipher stream generator to generate a key used to encrypt the plaintext message. See col. 6, lines 1-16. Hence, the shared private key in the Wright reference is not randomly generated and instead appears to be a calculated value based on the inputs of y , a , p and PK .

Accordingly, the Wright reference does not teach or even suggest the various features of claim 1 including providing a secret random binary encryption key provided by a key generator and recording the key on a first portable medium and a second portable medium so as to define a first and a second recorded key, a first user of the at least two users receiving the first portable medium with the first recorded key and a second user of the at least two users receiving the second portable medium with the second recorded key.

The Samar and Wright references together do not teach or even suggest ALL of the claim features of claim 1. That is, the Samar reference does not cure the deficiencies of the Wright reference. The Samar reference purportedly concerns a system and method to transparently integrate private key operations from a smart card with host-based encryption services. Title. The Samar reference refers to a system and method for providing transparent integration of a smart card private key operations with an existing set of encryption services and system applications. Abstract, lines 1-3. The Samar reference further refers to a key store manager managing user key data and handling requests for key operations from the system applications; a user information file stores user data, including user private keys for users that do not have smart cards, and an indication of those users that have smart cards. Abstract, lines 3-8. The Samar reference refers to the set of system applications interfacing with the key store manager through encryption protocol specification application programming interfaces – where users connect to the system through terminals or remote computers that may be equipped with smart card readers. Abstract, lines 8-12. The Samar reference states that for users having smart cards, the key store manager forwards to the smart cards requests for private key operations, such as encryption or decryption with the user's private key, from the system applications. – in this manner, according to the Samar reference, the user's private key cannot be compromised by exposure to the computer system. Abstract, lines 12-18. The Samar reference states that for users without smart cards, the key store manager

forwards the request for private key operation to an encryption service for handling.

Abstract, lines 18-20.

In contrast to claim 1, the Samar reference does not teach or even suggest providing a secret random binary encryption key provided by a key generator and recording the key on a first portable medium and a second portable medium so as to define a first and a second recorded key, a first user of the at least two users receiving the first portable medium with the first recorded key and a second user of the at least two users receiving the second portable medium with the second recorded key, as in claim 1. Instead, the Samar reference appears to focus on integrating the key store manager with a plurality of smart cards. In the Samar reference, apparently a computer system incorporates both the key store manager and a number of smart cards by providing a path between the key store manager and any of the smart cards available on the computer system; the key store manager including a set of interfaces to the smart cards that allow it to facilitate communication between the system applications and the smart cards for handling private key based operations. Col. 2, line 60 - col. 3, line 2.

Further, there is no motivation to combine the Wright reference and the Samar reference in the present case. The Wright reference appears to concern the encryption of data packets using a sequence of private keys generated from a public key exchange, whereas the Samar reference appears to concern providing a smart card with a private key stored internally and which performs encryption and decryption itself. Accordingly, Applicants respectfully submit that the Wright and Samar references, alone or in combination, do not teach or suggest the various features of claim 1.

Claim 13 contains features analogous to those of claim 1; thus, claim 13 is allowable for essentially the same reasons as claim 1. Withdrawal of the rejection of claim 13 under 35 U.S.C. § 103(a) is respectfully requested. Remaining claims 2, 3, 7 to 11, 14, 18 and 19 depend from one of claim 1 and claim 13. Thus, those claims are allowable for at least essentially the same reasons as either claim 1 and claim 13.

In a previous Office Action, claims 4, 5, 15 and 16 were rejected under 35 U.S.C. § 103(a) as unpatentable over the Wright reference in view of the Samar reference and further in view of U.S. Patent No. 5,307,410 to Bennett (the "Bennett reference") as

supported by Menezes et al., “Handbook of Applied Cryptography,” 1997, CRC Press, pages 171-173 (the “Menezes reference”).

Claims 4, 5, 15 and 16 depend from one of claims 1 and 13. As explained above, the Wright and Samar references, alone or in combination, do not teach or suggest at least the features of providing a secret random binary encryption key provided by a key generator and recording the key on a first portable medium and a second portable medium so as to define a first and a second recorded key, a first user of the at least two users receiving the first portable medium with the first recorded key and a second user of the at least two users receiving the second portable medium with the second recorded key, as in claim 1.

The Bennett reference does not cure the deficiencies of the Wright and Samar references. The Bennett reference purportedly concerns an interferometric quantum cryptographic key distribution system incorporating a quantum channel for conveying dim and reference light pulses, a timing channel, a source of coherent light pulses, beamsplitters, a random number generator, a phase modulator and a memory for recording the phase of transmitted dim light pulses. Abstract, lines 1-7. The Bennett reference refers to overcoming the problem of distributing fresh cryptographic key information between two users who share no secret information initially. Abstract, lines 11-14. The Bennett reference further refers to having a plurality of communication nodes, a second timing channel for conveying timing signals connected to the second port of the plurality of communication nodes, a third message channel for conveying information selected from the group consisting of plain text and encrypted text connected to the third port of the plurality of communication nodes. Col. 2, lines 41-52. The Bennett reference refers to distributing cryptographic key information from a first communication node to a second communication node comprising a first quantum channel for conveying dim and reference light pulses connected to the first and second communication nodes. Col. 3, lines 17-51. The Bennett reference does not teach or suggest at least the features of providing a secret random binary encryption key provided by a key generator and recording the key on a first portable medium and a second portable medium so as to define a first and a second recorded key, a first user of the at least two users receiving the first portable medium with the first recorded key and a second user of the at

least two users receiving the second portable medium with the second recorded key, as in claim 1.

The Menezes reference does not cure the deficiencies of the Wright, Samar and Bennett references. Instead, the Menezes reference is a text book which purportedly concerns random bit generation and states that a true random bit generator requires a naturally occurring source of randomness. Menezes, page 171. The Menezes reference refers to hardware-based generators stating that the hardware-based random bit generators exploit the randomness which occurs in some physical phenomena such as elapsed time between emission of particles during radioactive decay or thermal noise from a semiconductor diode or resistor, etc. Menezes, page 172. The Menezes reference further states that a generator based on such phenomena (elapsed time..., thermal noise...) would have to be built externally to the device using random bits and may be subject to observation or manipulation by an adversary. Menezes, page 172. The Menezes reference further states that pseudorandom bit generation, i.e., where a one way function f can be used to generate pseudorandom bit sequences by first selecting a random seed s , and then applying the function to the sequence of values $s, s+1, s+2, \dots$, such as the cryptographic hash function referred to has not been proven to be cryptographically secure, but appear sufficient for most applications. Menezes reference, page 173.

In fact, none of the Wright, Samar, Bennett and Menezes references teach or suggest at least the features of providing a secret random binary encryption key provided by a key generator and recording the key on a first portable medium and a second portable medium so as to define a first and a second recorded key, a first user of the at least two users receiving the first portable medium with the first recorded key and a second user of the at least two users receiving the second portable medium with the second recorded key, as in claim 1. Accordingly, the Wright, Samar, Bennett and Menezes references, alone or in combination, do not teach or suggest the features of claim 1, thus, it is respectfully submitted that claim 1 is allowable over the cited art.

Since claim 13 contains features analogous to those of claim 1, it is respectfully submitted that claim 13 is allowable over the cited art for essentially the same reasons as

claim 1. Since claims 4, 5, 15 and 16 depend from one of claims 1 and 13, it is respectfully submitted that claims 4, 5, 15 and 16 are allowable over the Wright, Samar, Bennett and Menezes references.

In a previous Office Action, claims 6 and 17 were rejected under 35 U.S.C. § 103(a) as unpatentable over the Wright reference in view of the Samar reference and further in view of the Menezes reference.

Claims 6 and 17 depend from one of claims 1 and 13. As explained above, the Wright, Samar and Menezes references, alone or in combination, do not teach or suggest at least the features of providing a secret random binary encryption key provided by a key generator and recording the key on a first portable medium and a second portable medium so as to define a first and a second recorded key, a first user of the at least two users receiving the first portable medium with the first recorded key and a second user of the at least two users receiving the second portable medium with the second recorded key, as in claim 1; thus, it is respectfully submitted that claim 1 is allowable over the cited art.

Since claim 13 contains features analogous to those of claim 1, it is respectfully submitted that claim 13 is allowable over the cited art for essentially the same reasons as claim 1. Since claims 6 and 17 depend from one of claims 1 and 13, it is respectfully submitted that claims 6 and 17 are allowable over the Wright, Samar and Menezes references.

In a previous Office Action, claim 12 was rejected under 35 U.S.C. § 103(a) as unpatentable over the Wright reference in view of the Samar reference and further in view of Schneier, "Applied Cryptography," 1996, John Wiley & Sons, 2nd ed., pages 197-199, 202, 203 (the "Schneier reference").

Claim 12 depends from claim 1. As explained above, the Wright and Samar references, alone or in combination, do not teach or suggest at least the features of providing a secret random binary encryption key provided by a key generator and recording the key on a first portable medium and a second portable medium so as to define a first and a second recorded key, a first user of the at least two users receiving the first portable medium with the first recorded key and a second user of the at least two users receiving the second portable medium with the second recorded key, as in claim 1.

The Schneier reference does not cure the deficiencies of the Wright and Samar references. Instead, the Schneier reference purportedly concerns stream ciphers which convert plaintext one bit at a time. Schneier, page 197. The Schneier reference refers to a systems' security depending entirely on the insides of a keystream generator which outputs a stream of bits because if the keystream generator outputs an endless stream of zeros, the ciphertext will equal the plaintext and the entire operation will be worthless (the keystream is XORed with a stream of plaintext bits to produce the stream of cipher bits. Id. The Schneier reference further refers to if the keystream generator spits out an endless stream of random (not pseudo-random) bits, you have a one-time pad and perfect security. Id. In fact none of the Wright reference, Samar reference and Schneier reference teach or suggest at least the features of providing a secret random binary encryption key provided by a key generator and recording the key on a first portable medium and a second portable medium so as to define a first and a second recorded key, a first user of the at least two users receiving the first portable medium with the first recorded key and a second user of the at least two users receiving the second portable medium with the second recorded key, as in claim 1. Accordingly, the Wright, Samar and Schneier references, alone or in combination, do not teach or suggest the features of claim 1, thus, it is respectfully submitted that claim 1 is allowable over the cited art.

Since claim 12 depends from claim 1, it is respectfully submitted that claim 12 is allowable over the Wright, Samar and Menezes references for at least the same reasons as claim 1.

Moreover, to reject a claim as obvious under 35 U.S.C. § 103, the prior art must describe or suggest each claim element and it must also provide a motivation or suggestion for modifying the elements in the manner contemplated by the claim. (See *Northern Telecom, Inc. v. Datapoint Corp.*, 908 F.2d 931, 934 (Fed. Cir. 1990), cert. denied, 111 S. Ct. 296 (1990). It is therefore respectfully submitted that the claims rejected as obvious are allowable over the references relied upon in the Office Action. Thus, it is respectfully submitted that all of claims 1 to 19 are allowable for the foregoing reasons.

New claim 20 depends from claim 13; thus, claim 20 is allowable for at least the same reasons as claim 13.

CONCLUSION

In view of all of the above, it is believed that any previously cited rejections have been obviated and should be withdrawn, and that all claims 1 to 20 are allowable. It is therefore respectfully requested that the present application issue as early as possible.

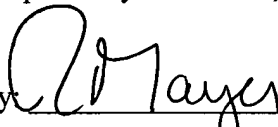
If for any reason the Examiner believes that contact with Applicants' attorney would advance the prosecution of this application, he or she is invited to contact the undersigned at the number given below.

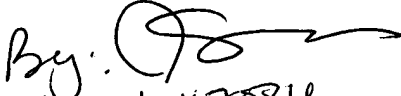
Dated: January 18, 2005

CUSTOMER NO. 26646

Respectfully submitted,

By


Richard L. Mayer (Reg. No. 22,490)
KENYON & KENYON
One Broadway
New York, New York 10004
(212) 425-7200 (telephone)
(212) 425-5288 (facsimile)

By: 
Reg No. 47084